Computing weight one modular forms over $\mathbf{C}$ and $\overline{\mathbf{F}}_p$.

Kevin Buzzard

March 4, 2013

Abstract

We report on a systematic computation of weight one cuspidal eigenforms for the group $\Gamma_1(N)$ in characteristic zero and in characteristic $p > 2$. Perhaps the most surprising result was the existence of a mod 199 weight 1 cusp form of level 82 which does not lift to characteristic zero.

Introduction

It is nowadays relatively easy to compute spaces of classical cusp forms of weights two or more, thanks to programs by William Stein written for the computer algebra packages Magma [BCP97] and SAGE [S$^+$12]. On the other hand, there seems to be relatively little published regarding explicit computations of weight one cusp forms. Computations have been done by Buhler ([Buh78]) and Frey and his coworkers ([Fre94]), and there is a beautiful paper of Serre ([Ser77]) which explains several tricks for computing with weight one forms of prime level, but as far as we know there is nothing systematic in the literature. In this paper we report on a fairly systematic computation of weight 1 forms that we did using MAGMA about ten years ago now. The characteristic zero code we wrote has since been incorporated as part of MAGMA, but the methods work just as well in characteristic p; indeed for a given level N we can compute mod p for all primes $p \nmid N$ at once (we do not even attempt to define mod p modular forms of level N if $p \mid N$). We apologise for our laziness in writing up these results. Our methods and calculations have in the mean time been greatly extended by George Schaeffer and forthcoming work of his will make our example of a non-liftable mod 199 form of level 82 look rather puny.

The methods basically go back to Buhler's thesis [Buh78], and the main idea is very simple: we cannot compute in weight 1 directly using modular symbols, but if we choose a non-zero form f of weight $k \geq 1$ then multiplication by f takes us from weight 1 to weight $k+1 \geq 2$ where we can compute using modular symbols, and then we divide by f again to produce the space of weight 1 forms with possible poles where f vanishes. Repeating this idea for lots of choices of f and intersecting the resulting spaces will often enable us to compute the space

of holomorphic weight 1 forms rigorously. We explain the details in the next section.

Recent developments by Khare and Wintenberger on Serre's conjecture give another approach for computing weight 1 forms in characteristic zero: instead of working on the automorphic side one can compute on the Galois side. The work of Khare and Wintenberger implies that there is a bijection between the set of weight 1 new eigenforms over $\mathbf{C}$ and the set of continuous odd irreducible representations $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ (see Théorème 4.1 of [DS74] for one direction and Corollary 10.2 of [KW09] for the other). Say ρ_f is the Galois representation attached to the form f; then the level of f is the conductor of ρ_f. Let us consider for a moment an arbitrary irreducible representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$. The projective image of ρ in $\mathrm{PGL}_2(\mathbf{C})$ is a finite subgroup of $\mathrm{PGL}_2(\mathbf{C})$ and is hence either cyclic, dihedral, or isomorphic to A_4, S_4 or A_5, and in fact the cyclic case cannot occur because ρ is irreducible. If f is a characteristic zero eigenform then we say that the *type* of f is dihedral, A_4, S_4 or A_5 according to the projective image of ρ_f. Because of the Khare–Wintenberger work, one approach for computing weight 1 modular forms of level N in characteristic zero would be to list all the finite extensions of $\mathbf{Q}$ which could possibly show up as the kernel of the projective representation attached to a level N form, and then reverse-engineer the situation (carefully analysing liftings and ramification, which would not be much fun) to produce the forms themselves. Listing the extensions is just about possible: one can use class field theory to deal with the dihedral cases, and the A_4, S_4 and A_5 calculations can be done because the projective representation attached to a level N form is unramified outside N, so to compute in level N one just has to list all A_4, S_4 and A_5 extensions unramified outside N (which is feasible nowadays for small N and indeed there are now tables of such things, see for example [JR] for an online resource). However lifting the projective representation to a representation can be troublesome to do in practice. Furthermore, this approach does not work in characteristic p: the problem is if k is a finite subfield of $\overline{\mathbf{F}}_p$ then $\mathrm{PGL}_2(k)$ is a finite subgroup of $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$, and this gives us infinitely many more extensions which must be checked for; hence the method breaks down. In fact looking for mod p Galois representations with large image is quite hard, it seems, and perhaps it is best to do the calculations on the automorphic side and use known theorems to deduce results on the Galois side. For example, as a consequence of our search at level 82 we proved the following result:

Theorem 1. *(a) There is a mod 199 weight 1 cusp form of level 82 which is not the reduction of a characteristic zero form.*

(b) There is a number field M, Galois over $\mathbf{Q}$, unramified outside 2 and 41, with Galois group $\mathrm{PGL}_2(\mathbf{Z}/199\mathbf{Z})$.

We prove this result in the final section.

When we initially embarked upon this computation, the kinds of things we wanted to know were the following:

- What are the ten (or so) smallest integers N for which the space of weight 1

cusp forms of level N is non-zero?

- What is the smallest N for which there exists a weight 1 level N eigenform whose associated Galois representation has projective image isomorphic to A_4? To S_4?
- Give some examples of pairs (N, p) consisting of an integer N and a prime p for which there is a mod p weight 1 eigenform of level N which does not lift to a characteristic zero eigenform of level N (Mestre had already given some examples when $p = 2$).

We found it hard to extract the answers to these questions from the literature, so we answered them ourselves with a systematic computation of weight one forms in characteristic zero and $p > 2$. We looked in the range $1 \leq N \leq 200$ in characteristic zero, and $1 \leq N \leq 82$ in characteristic p (adopting a "quit while you're ahead" policy). Both of these bounds are very modest and even ten years ago, when we actually did the calculations, it would have been possible to go further. George Schaeffer has since stepped up to the plate and his forthcoming PhD thesis pushes these calculations much further.

We did not find any characteristic zero weight 1 modular forms with associated Galois representations having projective image isomorphic to A_5 so we do not know what the smallest conductor of an A_5-representation is; as far as we know the smallest known conductor is Buhler's example, which has conductor 800.

The outline of this paper is as follows. We explain our algorithm in section 1, summarise the characteristic zero results in section 2, and the characteristic p results in section 3.

1 Computing weight one cusp forms.

We remind the reader of some definitions. If $N \geq 5$ is an integer, then there is a smooth affine curve $Y_1(N)$ over $\mathbf{Z}[1/N]$ parameterising elliptic curves over $\mathbf{Z}[1/N]$-schemes equipped with a point of exact order N. The fibres of $Y_1(N) \to \mathrm{Spec}(\mathbf{Z}[1/N])$ are geometrically irreducible. If $E_1(N)$ denotes the universal elliptic curve over $Y_1(N)$ then the pushforward of $\Omega^1_{E_1(N)/Y_1(N)}$ is a sheaf ω on $Y_1(N)$. There is a canonical compactification $X_1(N)$ of $Y_1(N)$, obtained by adding cusps, and this curve is smooth and proper over $\mathbf{Z}[1/N]$. Furthermore the sheaf ω extends in a natural way to $X_1(N)$. If R is any $\mathbf{Z}[1/N]$-algebra then we denote by $X_1(N)_R$ the pullback of $X_1(N)$ to R. We write $M_k(N; R)$ for $H^0(X_1(N)_R, \omega^{\otimes k})$ and refer to this space as the level N weight k modular forms defined over R. We write $S_k(N; R)$ for the sub-R-module of this R-module consisting of sections which vanish at every cusp.

If K is a field where N is invertible then the K-dimension of $M_k(N; K)$ is 0 if $k < 0$, it is 1 if $k = 0$, and can be easily computed if $k \geq 2$ using the Riemann–Roch formula. If however $k = 1$ then the Riemann–Roch theorem unfortunately only tells us the dimension of the subspace of Eisenstein series in $M_k(N; K)$.

Similarly for $k \neq 1$ the dimension of $S_k(N;K)$ is also easily computed, but for $k = 1$, even the dimensions of these spaces seem to lie deeper in the theory.

A weight one cusp form of level N is a section of ω which vanishes at every cusp, and is hence a section of $\omega \otimes C^{-1}$ where C is the sheaf associated to the divisor of cusps. One can compute the degree of ω on $X_1(N)_{\mathbf{C}}$ without too much trouble: for example $\omega^{\otimes 12}$ descends to a degree 1 sheaf on the j-line $X_0(1)_{\mathbf{C}}$ and hence the degree of ω on $X_1(N)$ is $[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_1(N)]/24$. Similarly the number of cusps on $X_1(N)_{\mathbf{C}}$ is well-known to be $\frac{1}{2}\sum_{0<d|N} \phi(d)\phi(N/d)$, the sum being over the positive divisors of N. Hence the degree of $\omega \otimes C^{-1}$ is easily computed in practice for small N. Although we did these calculations over $\mathbf{C}$, the degree of ω is the same in characteristic zero and in characteristic p (we are assuming $N \geq 5$ so the scheme of cusps over $\mathbf{Z}[1/N]$ is etale). From these formulae, which are messy but entirely elementary, it is easy to deduce the following.

Lemma 2. *Let K be a field in which the positive integer N is invertible. Then there are no non-zero weight 1 cusp forms of level N over K, if $5 \leq N \leq 22$, $24 \leq N \leq 28$, $N = 30$ or $N = 36$.*

Proof. Indeed, the degree of $\omega \otimes C^{-1}$ is less than zero in these cases. □

If $N \leq 4$ then there are theoretical issues with the approach we have adopted, because $X_1(N)_K$ is only a coarse moduli space, and there is no sheaf ω on $X_1(N)_K$ (there is a problem at one of the cusps when $N = 4$, and problems at elliptic points when $N \leq 3$). On the other hand, one can still give a rigorous definition of a modular form of level N for $N \leq 4$ (using the theory of algebraic stacks, for example, or the classical definition as functions on the upper half plane if $K = \mathbf{C}$) and one easily checks, using any of these definitions, that a cusp form of level N is also naturally a cusp form of level Nt for any positive integer t. Because 1,2,3 and 4 all divide 12, and there are no non-zero cusp forms of level 12 by the above lemma, we conclude

Corollary 3. *Let K be a field where the positive integer N is invertible. There are no non-zero cusp forms of level N over K for any $N < 23$.*

The same argument shows that the dimension of the space of weight 1 cusp forms of level 23 is at most 1, because the degree of $\omega \otimes C^{-1}$ on $X_1(23)$ is 0. Moreover, there will be a non-zero cusp form of level 23 if and only if this sheaf is isomorphic to the structure sheaf on $X_1(23)$. Conversely, there is indeed a non-zero level 23 weight 1 cusp form in characteristic zero: namely the form $\eta(q)\eta(q^{23})$, where $\eta = q^{1/24}\prod_{n\geq 1}(1-q^n)$. The mod p reduction of this form is a mod p cusp form for any $p \neq 23$, and this proves that the dimension of the level 23 forms is 1 in characteristic zero and in characteristic $p \neq 23$.

We have now solved the problem of computing weight one level N cusp forms for $N \leq 28$, but of course such tricks only work for small levels, and for $N \geq 29$ we used a computer to continue our investigations. Our strategy was as follows. Let K be an algebraically closed field where $N \geq 29$ is invertible. Let $S_k(N;K)$ denote the weight k cusp forms of level N defined over K. We wish

to compute $S := S_1(N;K)$. First let us choose a form $0 \neq f \in M_k(N;K)$ for some $k \geq 1$ that we can compute the q-expansion of to arbitrary precision (for example f can be a form of weight at least 2, or a weight 1 Eisenstein series or theta series). Then $f.S := \{fh : h \in S\}$ is a subspace of $S_{k+1}(N;K)$, which is a space that we can compute as $k+1 \geq 2$. We compute a basis of q-expansions for $S_{k+1}(N;K)$, and then divide each q-expansion by f, giving us an explicit finite-dimensional space of q-expansions which contains S. Repeating this for many choices of f and continually taking intersections will typically cut this space down, but after a while its dimension will stabilise. Let V be the space of q-expansions so obtained; this is now our candidate for S. We know for sure that it contains S. In fact, if we could somehow choose forms f_1 and f_2 as above, which were guaranteed to have no zeros in common on $X_1(N)_K$, then we would know for sure that our space really was S. However, we know of no efficient way of testing to see whether two given forms share a zero on $X_1(N)$, especially in characteristic p. Note that in [Fre94] they work over the complexes and do make a careful choice of f_1 and f_2, which they could prove had no common zero; our approach is more haphazard.

So far, we have a "candidate space" of q-expansions, which we know includes S and this gives us a reasonable upper bound for the dimension of S. To get a good lower bound, because we were only really interested in the case of N at most 200 or so, we wrote a program which counts dihedral representations. More precisely, what our program does is the following. For a given N it counts the number of representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ which are continuous, odd, irreducible, induced from a character of a quadratic extension of $\mathbf{Q}$, and have conductor N. This computation is a finite one because if M is a quadratic extension of $\mathbf{Q}$ and $\psi : \mathrm{Gal}(\overline{M}/M) \to \mathbf{C}^\times$ is a continuous 1-dimensional representation then the conductor of $\mathrm{Ind}(\psi)$ is the absolute value of $\mathrm{disc}(M)|c(\psi)|$, where $c(\psi)$ is the conductor of ψ (an ideal of the integers of M), and $|c(\psi)|$ is its norm. Hence there are only finitely many possibilities for M and, for each possiblity, one can use class field theory to enumerate the characters $\mathrm{Gal}(\overline{M}/M) \to \mathbf{C}^\times$ of conductor I, for I any ideal of $\mathcal{O}_M$. This approach gives a lower bound for the dimension of the space of newforms in S, and if we repeat the computation for divisors of N, then we get a lower bound for the dimension of S.

We have explained how to get both upper and lower bounds for the dimension of a space S of characteristic zero weight one cusp forms. If these bounds coincide, which of course they often do in practice in the range we considered, then we have computed the dimension of S, we have also proved that the Galois representations associated to all eigenforms of level N and conductor χ are induced from characters of index two subgroups, and furthermore, because both methods we have sketched are constructive, we now have two ways of actually computing the q-expansions of a basis for S to as many terms as we like, within reason – an automorphic method and a Galois method.

If however we run the algorithm above, and the lower bound it produces is still strictly less than our upper bound, then we guess that there are some non-dihedral forms at level N that are not contributing to our lower bound. What we

now need is a way of rigorously proving that these formal q-expansions really do correspond to holomorphic weight 1 forms rather than forms with poles. We do this as follows. Choose a form h in our vector space V. We are now suspecting that h is holomorphic; what we know is that $h = g/f$ for some non-zero weight k form f and weight $k+1$ form g. Let D denote the divisor of zeros of f. Then h is a meromorphic section of ω, with divisor of poles bounded by D. In particular we have a bound on the degree of the divisor of poles of h^2, which is now meromorphic and weight 2. Now here's the trick. If we can find a *holomorphic* weight 2 form ϕ of level N whose q-expansion is the same as that of h^2 up to order q^{M+1}, where M is a large integer, then we have *proved* that h^2 is holomorphic; for $h^2 - \phi$ is a weight 2 form which is a holomorphic section of $\omega^{\otimes 2} \otimes (2D) \cong \omega^{\otimes(2+2k)}$ and yet it has a zero of order at least M at ∞, so as long as M is greater than the degree of $\omega^{\otimes(2+2k)}$ the form $h^2 - \phi$ must be identically zero, and in particular h must be holomorphic. If we can prove that a basis for V consists of holomorphic forms, then we have proved $V = S$. If this algorithm fails then we have really proved $V \neq S$ and we go back to choosing forms f as above and dividing out. Eventually in practice the process terminates, at least for $N \leq 200$ or so on architecture that is now ten years old. As mentioned before, George Schaeffer has taken all of this much further now.

In practice we do not quite do what is suggested above. Firstly, instead of working with the full space of forms of level N we fix a Dirichlet character of level N and work with forms of level N and this character. This gives us a huge computational saving because it cuts down the dimension of all the spaces we are working with by a factor of (very) approximately N. It does introduce some thorny issues at primes dividing $\phi(N)$, where the diamond operators may not be semisimple, but these can be dealt with by simply gritting one's teeth and ignoring diamond operators whose order divides p in this case. In fact the issues became sufficiently thorny here for $p = 2$ that we decided to leave $p = 2$ alone and restrict to the case $p > 2$.

Secondly, in fact we do not work over a field at all; we do the entire calculation on the integral level, working over $\mathbf{Z}[\zeta_n]$ for ζ_n a primitive nth root of unity, n chosen sufficiently large that all the relevent Dirichlet characters showing up in the computation have order dividing n. In characteristic zero we only need to compute with one Dirichlet character per Galois conjugacy class; but a characteristic zero conjugacy class can break into several conjugacy classes mod p and so we need to reduce things not modulo p but modulo the prime ideals of $\mathbf{Z}[\zeta_n]$. If χ and α are $\mathbf{Z}[\zeta_n]$-valued Dirichlet characters of level N, and we are trying to compute in level N, weight 1 and character χ, then we choose $f \in S_k(N, \alpha; \mathbf{Z}[\zeta_n])$ and let L denote the lattice $S_{k+1}(N, \alpha\chi; \mathbf{Z}[\zeta_n])/f$. We run through many choices of f and, instead of intersecting vector spaces, we intersect lattices. When computing an intersection of two lattices L_1 and L_2 arising in the above way, one computes not just the intersection but also the size of the torsion subgroup of $(L_1 + L_2)/L_1$; if any prime number divides the order of this torsion subgroup then the intersection of L_1 and L_2 is bigger in characteristic p than in characteristic zero. The torsion subgroup is a $\mathbf{Z}[\zeta_n]$-module and we compute the primes above p in its support; the reduction of χ modulo

these prime ideals are the mod p characters where there may be more mod p forms than characteristic zero forms. Note that in practice the order of the torsion subgroup of $(L_1 + L_2)/L_1$ can be so big that it is unfactorable, but this does not matter because we simply collect all the orders of these torsion groups and continually compute their greatest common divisor. What often happens in practice is that we manage to prove that the intersection is no bigger in characteristic p than in characteristic zero for all odd $p \nmid N$; then we have proved that all characteristic p forms lift to characteristic zero.

Occasionally however we may run into a suspect prime number p which shows up in a lot of the torsion orders; we can then compute the q-expansion of our candidate non-liftable form and square it and look in weight 2 in characteristic p as explained above; if we can find the q-expansion of the square in weight 2 to sufficiently high precision then we have constructed a non-liftable form.

These tricks, put together, always worked in the region in which we did computations, which was $N \leq 200$ in characteristic 0 and $N \leq 82$ in characteristic $p > 2$. We stopped at $N = 200$ in characteristic zero because by then we had seen A_4 and S_4 extensions, but we still felt a long way from $N = 800$ (for which there is a known A_5 example) – there is no reason why one should not be able to proceed further nowadays however. In characteristic p we were running into problems of factoring very large integers when computing the torsion subgroups of the quotients above, so we stopped at $N = 82$ because of a very interesting example that we found there (see section 3).

2 Characteristic zero results.

We ran our calculations in characteristic 0 for all $N \leq 200$. Of course, the dimension of $S_1(N, \chi; \mathbf{C})$ was usually zero.

2.1 Small level.

In characteristic zero there is a good theory of oldforms and newforms, and we firstly list the dimensions of all the non-zero spaces $S_1^{\mathrm{new}}(N, \chi; \mathbf{C})$ for $N \leq 60$. Note that if χ_1 and χ_2 are Galois conjugate characters then the associated spaces $S_1^{\mathrm{new}}(N, \chi_1; \mathbf{C})$ and $S_1^{\mathrm{new}}(N, \chi_2; \mathbf{C})$ are also Galois conjugate in a precise sense, and in particular have the same dimension, so we only list characters up to Galois conjugacy. The (lousy) notation we use for characters is as follows: if the prime factorization of N is $p^e q^f \ldots$, then a Dirichlet character χ of level N can be written as a product of Dirichlet characters χ_p, $\chi_q \ldots$ of levels p^e, $q^f, \ldots$. By p_a we mean a character χ_p of level p^e and order a, and by $p_a q_b \ldots$ we mean the product of such characters. This notation will not always specify the Galois conjugacy class of a character uniquely (which is why it's lousy), but it does in the cases below apart from the case $N = 56$, where we need to add that the character 2_2 is the unique even character of level 8 and order 2 (thus making the product $2_2 7_2$ odd).

N	χ	dimension of $S_1(N, \chi; \mathbf{C})$
23	23_2	1
31	31_2	1
39	$3_2 13_2$	1
44	$2_1 11_2$	1
47	47_2	2
52	$2_2 13_3$	1
55	$5_2 11_2$	1
56	$2_2 7_2$	1
57	$3_2 19_3$	1
59	59_2	1

One can now deduce, for example, that the dimension of $S_1(52; \mathbf{C})$ is two, because the character in the table above has a non-trivial Galois conjugate, and both the character and its conjugate contribute 1 to the dimension. All of these forms are of dihedral type and hence are easily explained in terms of ray class groups. For example, the two newforms at level 47 are explained by the fact that the class group of $L = \mathbf{Q}(\sqrt{-47})$ is cyclic of order 5, and if H denotes the Hilbert class field of L then the four non-trivial characters of $\mathrm{Gal}(H/L)$ can all be induced up to give 2-dimensional Galois representations of $\mathrm{Gal}(H/\mathbf{Q})$ of conductor 47 (one gets two isomorphism classes of 2-dimensional representations). In particular, the two newforms of level 47 are defined over $\mathbf{Q}(\sqrt{5})$ and are Galois conjugates. As another example, one checks that if P is a prime above 13 in $\mathbf{Q}(i)$ then the corresponding ray class field of conductor P has degree 3 over $\mathbf{Q}(i)$, and the corresponding order 3 character of the absolute Galois group of $\mathbf{Q}(i)$ can be induced up to $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ giving a 2-dimensional representation of conductor 52 which is readily checked to be irreducible and odd, and is the representation corresponding to the level 52 form in the table above.

One can of course also explain all the forms in the table above using theta series: for example the first form in the list has level 23 and quadratic character; the corresponding normalised newform f can be written down explicitly: $2f = \sum_{m,n} q^{m^2+mn+6n^2} - q^{2m^2+mn+3n^2}$. There is also another well-known formula for f, namely $f = \eta(q)\eta(q^{23})$, where $\eta(q) = q^{1/24}\prod_n(1-q^n)$. For other examples one can see [Ser77].

2.2 Non-dihedral examples.

Our algorithm computed lower bounds for spaces of forms by counting dihedral representations, and hence our methods make it easy to spot when one has discovered a form which is not of dihedral type. To work out what is going on with these forms one needs to do both local and global calculations; the more pedantic amongst us might at this point like to choose algebraic closures $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, and $\overline{\mathbf{Q}}_\ell$ of $\mathbf{Q}_\ell$ for all primes ℓ, and also embeddings of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_\ell$ (for all ℓ) and into $\mathbf{C}$; this makes life slightly easier in terms of notation.

Notation: if ℓ is a prime then D_ℓ denotes the absolute Galois group of $\mathbf{Q}_\ell$,

and I_ℓ is its inertia subgroup.

The smallest level where there is a non-dihedral form is $N = 124 = 2^2 \times 31$. In fact at level 124 there are four non-dihedral newforms (and no other newforms, although there is a 3-dimensional space of oldforms coming from level 31). Let χ be a level 124 Dirichlet character with order 2 at 2 and order 3 at 31; then $S_1(124, \chi; \mathbf{C})$ has dimension 2, as does $S_1(124, \chi^c; \mathbf{C})$ where χ^c denotes the complex conjugate of χ. What are the Galois representations attached to the corresponding eigenforms? Well, let f, g denote the two normalised eigenforms in $S_1(124, \chi; \mathbf{C})$.

Lemma 4. *The projective image of the Galois representations associated to f and g are isomorphic to A_4; furthermore, in both cases the number field cut out by this projective representation is the splitting field K of $x^4 + 7x^2 - 2x + 14$.*

Proof. We use the following strategy. We first construct two odd Galois representations to $\mathrm{GL}_2(\mathbf{C})$ of conductor 124 and determinant χ, whose projective images both cut out K; such representations must come from weight 1 forms of level 124 and hence they must be the representations associated to f and g. The lemma is hence reduced to the construction of these two Galois representations, the heart of the matter being controlling the conductor. The strategy for doing such things is already in [Fre94]; a convenient reference is the Theorem (due to Tate) in §1 of [Kim94], which states that if we have a projective representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ and for each ramified prime ℓ with associated decomposition group D_ℓ we choose a lifting of $\overline{\rho}|D_\ell$ to $\rho_\ell : D_\ell \to \mathrm{GL}_2(\mathbf{C})$, then there is a global lift $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ of $\overline{\rho}$ such that if I_ℓ is the inertia subgroup of D_ℓ then $\rho|I_\ell \cong \rho_\ell|I_\ell$. In particular the conductor of ρ is the product of the conductors of the ρ_ℓ. This result reduces the computation of conductors of global lifts to a local calculation, which we now do.

The splitting field K has degree 12 over $\mathbf{Q}$. Let $\overline{\rho} : \mathrm{Gal}(K/\mathbf{Q}) \to \mathrm{PGL}_2(\mathbf{C})$ be an injection. We will lift $\overline{\rho}$ to ρ with conductor 124. One easily checks using a computer algebra package that K is unramified outside 2 and 31. The decomposition group at 2 is cyclic of order 2 and the completion of K at a prime above 2 is isomorphic to $\mathbf{Q}_2(\sqrt{3})$. The decomposition group at 31 is cyclic of order 3 and cuts out a ramified degree 3 extension K_{31} of $\mathbf{Q}_{31}$. The projective representation on the decomposition group at 2 lifts to a reducible representation $1 \oplus \tau$, with τ the order 2 local character which cuts out $\mathbf{Q}_2(\sqrt{3})$. This local representation has conductor 4. Similarly the projective representation at 31 lifts to the reducible representation $1 \oplus \sigma$, with σ an order 3 character with kernel corresponding to K_{31}. This local representation has conductor 31. Tate's theorem now implies that there is a global lift $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ of $\overline{\rho}$ with conductor 124, which furthermore on I_2 looks like $1 \oplus \tau$. We know that ρ is not induced from an index 2 subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ (if it were then the projective image of ρ would be dihedral), and hence $\rho' := \rho \otimes \chi_4 \not\cong \rho$, where χ_4 is the conductor 4 Dirichlet character. A local calculation at 2 shows that ρ' also has conductor 4 (note that $\mathbf{Q}_2^{nr}(\sqrt{3}) = \mathbf{Q}_2^{nr}(\sqrt{-1})$). Furthermore, ρ and ρ' are odd (because K is not totally real) and hence both modular, so correspond to two distinct newforms of level 124; these forms must be f and g. □

Note that the strategy of the above proof easily generalises to other levels, assuming one can find the relevant number field, which we could do in every case that we tried simply by looking through tables of number fields of small degree unramified outside a given set of primes. The next level where we see non-dihedral forms is $N = 133 = 7.19$, with character χ of order 2 at 7 and 3 at 19; again this determines χ up to conjugation. The weight 1 forms and the corresponding representations were originally discovered by Tate and some of his students in the 1970s; see the concluding remarks of [Tat76] for some more historical information about the calculations (which were done by hand)[1]. Again the dimension of the space of weight 1 forms of level N and character χ is 2, both forms are of A_4 type and the corresponding A_4-extension of $\mathbf{Q}$ is the splitting field of $x^4 + 3x^2 - 7x + 4$. This can be proved using the same techniques as the preceding lemma; the splitting field is unramified outside 7 and 19, the decomposition group at 7 is cyclic of order 2 cutting out $\mathbf{Q}_7(\sqrt{7})$ and the decomposition group at 19 is cyclic of order 3; the global quadratic character one twists by to get the second form is the one with conductor 7.

The next non-dihedral newform occurs at level $148 = 2^2 \times 37$, and it is our first form of type S_4. If χ is a Dirichlet character of level 148 which is trivial at 2 and has order 4 at 37 (there are two such characters, and they are Galois conjugate) then the dimension of $S_1(148, \chi; \mathbf{C})$ is 1. One checks using similar techniques that the S_4-extension of $\mathbf{Q}$ cut out by the projective Galois representation must be the splitting field of $x^4 - x^3 + 5x^2 - 7x + 12$. Indeed, the splitting field of this polynomial has Galois group S_4, is unramified outside 2 and 37, the decomposition group at 2 is isomorphic to S_3 with inertia the order 3 subgroup, and the decomposition and inertia groups at 37 are both cyclic of order 4. Note that any inclusion $S_3 \to \mathrm{PGL}_2(\mathbf{C})$ lifts to an inclusion $S_3 \to \mathrm{GL}_2(\mathbf{C})$; the induced map $\rho_2 : D_2 \to \mathrm{GL}_2(\mathbf{C})$ has conductor 4 because it is the sum of two order three tame characters on inertia.

The author confesses that he was initially slightly surprised to see this latter extension show up again in the next section.

3 Unliftable mod p weight 1 forms.

Of perhaps more interest are the mod p forms of level N that do not lift to characteristic 0 forms of level N. We first note the following subtlety: there is a mod 3 form of level 52 with character of order 2 at 2 and trivial at 13, and this mod 3 form does not lift to a characteristic zero cusp form with order 2 character. But this is not surprising – indeed this phenomenon can happen in weight $k \geq 2$ as well, and in weight 2 it first happens at $N = 13$; this was the reason that Serre's initial predictions about the character of the form giving rise to a modular representation needed a slight modification. The weight 1 mod 3 form of level 52 in fact lifts to a level 52 form with character of order 6, and also to an Eisenstein series of level 52 with order 2 character; on the Galois side what is happening is that the weight 1 level 52 cusp form of dihedral type

[1] We thank Chandan Singh Dalawat for pointing out this reference to us on MathOverflow.

mentioned in the previous section has associated Galois representation which is irreducible and induced from an index 2 subgroup, but the mod 3 reduction of this representation is reducible. The phenomenon of not being able to lift characters in an arbitrary manner was deemed "uninteresting" and we did not explicitly search for it (it happens again mod 5 at level 77 and many more times afterwards; note in particular that it can happen mod p for $p \geq 5$).

We now restrict our attention to mod p weight 1 eigenforms of level N which do not lift to characteristic zero eigenforms of level N. We did an exhaustive search for such examples with $p > 2$. The first example we found was at level 74, where there is a mod 3 form with character trivial at 2 and of order 4 at 37. The associated mod 3 Galois representation was checked to be irreducible and have solvable image, and this confused the author for a while, because he was under the impression that the only obstruction to lifting weight 1 forms was lifting the image of Galois. This notion is indeed vaguely true, but what is happening here is that the mod 3 form of level 74 lifts to no form of level 74 but to the form of type S_4 and level $148 = 2 \times 74$ which we described in the previous section. Why has the conductor gone up? It is for the following reason: there is a 2-dimensional mod 3 representation of D_2 whose image is the subgroup $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ of $\mathrm{GL}_2(\mathbf{F}_3)$ and such that the image of inertia has order 3. The conductor of this mod 3 representation is 2^1; however all lifts of this representation to $\mathrm{GL}_2(\mathbf{C})$ have conductor at least 2^2. This example was nice to find, not least because it gave the author confidence that his programs were working, as well as emphasizing just how miraculous this whole theory is – these subtleties of conductors dropping show up on both the automorphic side and the Galois side.

What we now realised we really wanted was a mod p form which did not lift to any weight 1 form at all. Fortunately we soon found it – it was at level $N = 82 = 2 \times 41$, and to our surprise was a mod 199 form (note that 199 is prime) whose associated Galois representation had rather large image. We finish this note by explaining what we found here.

Let $\mathbf{F}_{199^2}$ denote the field with 199^2 elements. Fix a root τ of $X^2+127X+1$; changing τ will just change everything below by the non-trivial field automorphism of $\mathbf{F}_{199^2}$. One can check that the multiplicative order of τ is 40.

Let χ be the group homomorphism $(\mathbf{Z}/82\mathbf{Z})^\times \to \mathbf{F}_{199^2}^\times$ which sends $47 \in (\mathbf{Z}/82\mathbf{Z})^\times$ (note that 47 is a generator of the cyclic group $(\mathbf{Z}/82\mathbf{Z})^\times$) to τ. Our programs showed that the space of mod 199 weight 1 cusp forms of level N and character χ was 1-dimensional. Let f denote this weight 1 eigenform. The reader who wants to join in at home will need to know the first few terms in the q-expansion of f:

$$\begin{aligned} f =& q + (18\tau + 85)q^2 + (183\tau + 55)q^3 + (120\tau + 135)q^4 + (171\tau + 45)q^5 \\ &+ (187\tau + 187)q^6 + (140\tau + 128)q^7 + (194\tau + 161)q^8 + (84\tau + 141)q^9 \\ &+ (151\tau + 150)q^{10} + (106\tau + 4)q^{11} + (127\tau + 191)q^{12} + (112\tau + 92)q^{13} \\ &+ (27\tau + 2)q^{14} + (146\tau + 37)q^{15} + (172\tau + 44)q^{16} + (192\tau + 4)q^{17} \\ &+ (137\tau + 125)q^{18} + (189\tau + 117)q^{19} + O(q^{20}) \end{aligned}$$

This is enough to determine f uniquely. For one can formally multiply this power series by a weight 1 Eisenstein series of level 82 and character χ^{-1} and the resulting q-expansion (which at this point we know up to $O(q^{20})$) is the q-expansion of a level 82 mod 199 weight 2 form with trivial character which turns out to be determined uniquely by the first 19 coefficients of its q-expansion. The q-expansion of this unique weight 2 form can be worked as far as one wants within reason; we computed it to $O(q^{20000})$ in just a few minutes. Dividing through by the Eisenstein series again gives us the q-expansion of f to as much precision as one wants.

Computing the q-expansion of f to high precision gives us, for free, plenty of facts about the mod 199 Galois representation associated to f. Note first that there *is* a mod 199 Galois representation attached to f; one can multiply f by the mod 199 Hasse invariant A to get a mod 199 form Af of weight 199 which is an eigenvector for all Hecke operators away from 199; the smallest Hecke-stable subspace containing Af is 2-dimensional and consists of two eigenvectors f_1 and f_2; the T_ℓ-eigenvalues of f, f_1 and f_2 all coincide for $\ell \neq 199$, and the T_{199}-eigenvalues of f_1 and f_2 are the two roots of $X^2 - a_{199}X + \chi(199)$, which are distinct. Both f_1 and f_2 lift to characteristic zero forms which are ordinary at 199, and the associated mod 199 Galois representations are isomorphic; this is the mod 199 Galois representation ρ_f associated to f.

It follows from the computation that the q-expansion of f has all coefficients in $\mathbf{F}_{199^2}$. Write $f = \sum_{n\geq 1} a_n q^n$, with $a_n \in \mathbf{F}_{199^2}$. Explicit computation shows that a_2 and a_{41} are non-zero. The Brauer group of a finite field is trivial and hence there is an associated semisimple Galois representation $\rho_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_{199^2})$. Standard facts about the mod p Galois representations associated to modular forms now imply that ρ_f is unramified outside $\{2, 41\}$. Indeed, for $\ell \neq 199$ this is standard, and for $\ell = 199$ we use the fact thet the mod 199 representations of D_{199} attached to f_1 and f_2 are upper triangular with unramified characters on the diagonal, and furthermore the unramified character showing up as the subspace in ρ_{f_1} is the character that shows up as the quotient in ρ_{f_2}; hence ρ_f restricted to D_{199} is a direct sum of two unramified characters, $\rho_f(\mathrm{Frob}_{199})$ is semisimple, and the characteristic polynomial of $\rho_f(\mathrm{Frob}_{199})$ is $X^2 - a_{199}X + \chi(199)$, just as the characteristic polynomial of $\rho_f(\mathrm{Frob}_\ell)$ is $X^2 - a_\ell X + \chi(\ell)$ for all other primes $\ell \notin \{2, 41\}$.

Standard mod p local-global results apply to f_1 and f_2, because they have weight bigger than 1 and lift to characteristic zero. Furthermore there are no weight 1 mod 199 forms of level 41 and character χ, hence ρ_f must be

ramified at 2 and at 41 (we are in a situation here where level-lowering results are known; indeed they are known for f_1 and f_2, which suffices because we shall show below that ρ_f is absolutely irreducible). The kernel of ρ_f hence corresponds to a number field L ramified only at 2 and 41 such that $\mathrm{Gal}(L/\mathbf{Q})$ is isomorphic to the image of ρ_f, which is a subgroup of $\mathrm{GL}_2(\mathbf{F}_{199^2})$. The local representation at 2 is Steinberg, which means that inertia at 2 has order 199; the local representation at 41 is principal series corresponding to one unramified and one tamely ramified (but ramified) character, which implies that inertia at 41 has order 40. In particular L is tamely ramified at both 2 and 41.

The only natural question left is: what is the image of ρ_f, or equivalently what is $\mathrm{Gal}(L/\mathbf{Q})$? For several years we assumed that the image would contain $\mathrm{SL}_2(\mathbf{F}_{199^2})$, but it was only in 2009 that we actually tried to sit down and compute it, and we discovered that in fact the image is smaller.

Proposition 5. *The image X of ρ_f is, after conjugation in $\mathrm{GL}_2(\overline{\mathbf{F}}_{199})$ if necessary, contained in $Z \cdot \mathrm{GL}_2(\mathbf{F}_{199})$, with Z the subgroup of scalar matrices in $\mathrm{GL}_2(\mathbf{F}_{199^2})$. Furthermore the quotient of X by $X \cap Z$ is $\mathrm{PGL}_2(\mathbf{F}_{199})$.*

Corollary 6. *(i) There is a number field M, Galois over $\mathbf{Q}$, unramified outside 2 and 41, tamely ramified at 2 and 41, and with $\mathrm{Gal}(M/\mathbf{Q}) = \mathrm{PGL}_2(\mathbf{F}_{199})$.*

(ii) The weight 1 form f does not lift to any weight 1 eigenform of characteristic zero.

Proof. (of corollary) (i) M is the kernel of $\overline{\rho}_f$. (ii) There is no finite subgroup of $\mathrm{GL}_2(\mathbf{C})$ with a subquotient isomorphic to the simple group $\mathrm{PSL}_2(\mathbf{F}_{199})$ and so ρ_f does not lift to $\mathrm{GL}_2(\mathbf{C})$; hence neither does f. □

Remark 7. The proof of the proposition involves a lot of machine computation and in fact, the proof we present here involves far more machine computation than all of the other computations of the paper put together. Computing all the forms in characteristic zero and characteristic p mentioned in this paper only took a day or two in 2002; proving the above proposition rigorously took several weeks of machine time (on a standard desktop running Debian linux and magma) in 2009.

Proof. (of Proposition) Let $\overline{\rho}_f$ denote the projective representation associated to ρ_f, so $\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{PGL}_2(\mathbf{F}_{199^2})$. It suffices to prove that the image of $\overline{\rho}_f$ is the subgroup $\mathrm{PGL}_2(\mathbf{F}_{199})$ of $\mathrm{PGL}_2(\mathbf{F}_{199^2})$. We now adopt a rather brute force approach. We have defined X to be the image of ρ_f; we now let $\overline{X}$ denote the image of $\overline{\rho}_f$ in $\mathrm{PGL}_2(\mathbf{F}_{199^2})$. The finite subgroups of $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ for p a prime were classified by Dickson (see [Dic58], sections 255 and 260); they are as follows. They are either conjugate in $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ to a subgroup of the upper-triangular matrices, are dihedral of order prime to p, are isomorphic to A_4, S_4 or A_5, or are conjugate to $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k)$ for some finite subfield $k \subset \overline{\mathbf{F}}_p$. We will rule out all but one possibility for $\overline{X}$; we know of no other way of proving the result. Ruling out $\mathrm{PSL}_2(\mathbf{F}_{199^2})$ will not be much fun at all.

We start by observing that looking at the q-expansion of f gives upper and lower bounds for the size of $\overline{X}$. First, the size of $\overline{X}$ is bounded above

by the size of $\mathrm{PGL}_2(\mathbf{F}_{199^2})$, and this means that $\overline{X}$ cannot be conjugate to $\mathrm{PSL}_2(k)$ or $\mathrm{PGL}_2(k)$ for any finite field k of size at least 199^3. In fact because $\det(\rho_f) = Im(\chi) = \mu_{40} \subset \mathbf{F}_{199^2}$ consists of squares in $\mathbf{F}_{199^2}$, the image of ρ_f is contained within $\mu_{80}\,\mathrm{SL}_2(\mathbf{F}_{199^2})$ (where here μ_{80} is the cyclic group of 80th roots of unity considered as a subgroup of the scalars in $\mathrm{GL}_2(\mathbf{F}_{199^2})$), which rules out the case $\overline{X} = \mathrm{PGL}_2(\mathbf{F}_{199^2})$ as well.

On the other hand we can compute the semisimple conjugacy classes of the first 1500 unramified primes by explicitly computing the q-expansion of f to high precision; this only takes a few minutes and shows that $\overline{X}$ has at least 199 elements (the point being that $a_\ell^2/\chi(\ell)$ takes on all 199 values of $\mathbf{F}_{199}$ as ℓ varies over the first 1500 unramified primes; we do not need to worry about whether Frobenii actually are semisimple, because if $g \in X \subseteq \mathrm{GL}_2(\mathbf{F}_{199^2})$ is non-semisimple then its semisimplification is $g^{199^2} \in X$). This means that $\overline{X}$ cannot be isomorphic to A_4, S_4 or A_5. Next we observe that $\overline{X}$ cannot be conjugate to a subgroup of the upper-triangular matrices. For if it were, the semisimple representation ρ_f would be the sum of two characters each having conductor a divisor of 82 and in particular one could deduce that if ℓ_1 and ℓ_2 were unramified primes which were congruent mod 82 then a_{ℓ_1} and a_{ℓ_2} would be equal; however this is not the case, as $a_7 \neq a_{89}$. As a consequence we deduce that ρ_f is absolutely irreducible.

We are left with the following possibilities: $\overline{X}$ can be dihedral of order prime to 199, or conjugate to $\mathrm{PSL}_2(k)$ for k of size 199 or 199^2, or conjugate to $\mathrm{PGL}_2(\mathbf{F}_{199})$. We next rule out the dihedral case; if $\overline{X}$ were dihedral then ρ_f restricted to an index two subgroup would be the sum of two characters, and hence ρ_f would be induced from an index 2 subgroup corresponding to a quadratic extension of $\mathbf{Q}$ unramified outside 2 and 41. There are only seven such extensions, namely $\mathbf{Q}(\sqrt{D})$ for $D \in \{2, 41, 82, -1, -2, -41, -82\}$, and for each one it is easy to find a prime $\ell \notin \{2, 41\}$ which is inert in the extension and such that $a_\ell \neq 0$ (indeed the smallest prime ℓ such that $a_\ell = 0$ is $\ell = 193$, but there is an inert prime $p \leq 13$ in each of these quadratic extensions). However all such Frobenius elements would have trace zero if X were dihedral.

We next rule out the case $\overline{X} = \mathrm{PSL}_2(\mathbf{F}_{199^2})$. The only method we know requires some serious computations. We have our weight 1 form $f = \sum_n a_n q^n$. Let $\psi : (\mathbf{Z}/41\mathbf{Z})^\times \to \mathbf{F}_{199^2}^\times$ be an arbitrary group homomorphism; there are 40 choices for ψ. Extend ψ to a map $\mathbf{Z} \to \mathbf{F}_{199^2}$ by defining $\psi(n) = 0$ if $41|n$. We claim that the q-expansion $f_\psi = \sum_{n\geq 1} \psi(n) a_n q^n$ is a mod 199 modular form of level 2×41^2. For ψ the trivial character this follows because $f_\psi(q) = f(q) - a_{41} f(q^{41})$. For non-trivial ψ this follows because the weight 199 forms f_1 and f_2 lift to characteristic zero forms which are ramified principal series at 41 (with one tamely ramified and one unramified character), and the twists of the lifts by the Teichmueller lift of ψ hence have level 2×41^2 and their q-expansions differ mod 199 only at coefficients q^n with $199|n$; the difference of the twists of the lifts then reduces to a mod 199 form which has q-expansion which is a power series in q^{199} and is hence the 199th power of a weight 1 form (by part (3) of the main theorem of [Kat77]) whose Galois conjugate is f_ψ.

Hence the form $g := \sum_{t\geq 0} a_{1+41t} q^{1+41t}$ is a mod 199 weight 1 modular form of level $2 \times 41^2 = 3362$, it being a linear combination of the f_ψ. Note that this form is *not* an eigenform for the diamond operators, which is what makes the computation non-trivial. We know $a_{1+41t} \in \mathbf{F}_{199^2}$ for all $t \geq 0$; we claim that in fact $a_{1+41t} \in \mathbf{F}_{199}$ for all $t \geq 0$. This can be verified with the following horrendous computation, which took nearly a month to do; if $a_{1+41t} \notin \mathbf{F}_{199}$ for some t then g would not be equal to its Galois conjugate $\overline{g}$, and hence $g - \overline{g}$ would be a non-zero mod 199 modular form of level 3362. However, one can check on a computer (given a month) that $a_{1+41t} \in \mathbf{F}_{199}$ for $0 \leq t \leq 8610$ and hence $g - \overline{g}$ has a zero at the cusp infinity of order at least 353011. However the degree of ω on $X_1(3362)$ is 353010 and hence $g - \overline{g}$ must be identically zero. The reason one needs to go so far is that one has to work with the whole of $X_1(3362)$ rather than the far smaller $X_0(3362)$, because g is not an eigenform for the diamond operators.

The conclusion so far is that $a_{1+41t} \in \mathbf{F}_{199}$ for all $t \geq 0$. In particular, if $\ell \equiv 1 \bmod 41$ is prime then the trace of $\rho_f(\mathrm{Frob}_\ell)$ is in $\mathbf{F}_{199}$. Set $K = \mathbf{Q}(\zeta_{41})$; then K is the field cut out by $\det(\rho_f)$ and in particular $K \subseteq L$, the field cut out by ρ_f. We regard ρ_f as a representation of $\mathrm{Gal}(L/\mathbf{Q})$ and we now consider its restriction to $\mathrm{Gal}(L/K)$. The Frobenius conjugacy classes corresponding to primes of K lying above rational primes $\ell \equiv 1 \bmod 41$ cover $\mathrm{Gal}(L/K)$, and the Brauer group of a finite field is trivial; we deduce that the restriction of ρ_f to $\mathrm{Gal}(L/K)$ can be conjugated within $\mathrm{GL}_2(\overline{\mathbf{F}}_{199})$ so that it lands within the subgroup $\mathrm{GL}_2(\mathbf{F}_{199})$. In fact because K is the field cut out by $\det(\rho_f)$ we see that $Y := \rho_f(\mathrm{Gal}(L/K))$ lands in $\mathrm{SL}_2(\mathbf{F}_{199})$ and in particular the size of $\rho_f(\mathrm{Gal}(L/K))$ is at most the size of $\mathrm{SL}_2(\mathbf{F}_{199})$ and hence is most $199^3 + 199$. Hence the size of $X = \rho_f(\mathrm{Gal}(L/\mathbf{Q}))$ is at most $40(199^3+199)$, which is hence an upper bound for X. This upper bound is far smaller than the size of $\mathrm{PSL}_2(\mathbf{F}_{199^2})$ which can hence be ruled out.

We finally have to distinguish between the two remaining possibilities for $\overline{X}$, namely $\overline{X} = \mathrm{PSL}_2(\mathbf{F}_{199})$ and and $\overline{X} = \mathrm{PGL}_2(\mathbf{F}_{199})$. Because $\overline{X}$ can be no larger than $\mathrm{PGL}_2(\mathbf{F}_{199})$ we do know that (after conjugation if necesary) $X \subseteq Z.\mathrm{GL}_2(\mathbf{F}_{199})$, with Z the scalars in $\mathrm{GL}_2(\mathbf{F}_{199^2})$. Furthermore $\det(X) = \mu_{40} \subset \mathbf{F}_{199^2}^\times$ and hence $X \cap Z \subseteq \mu_{80}$. One checks that if ℓ is the prime 661 then $\rho_f(\mathrm{Frob}_\ell)$ has semisimplification a scalar matrix with order 40 and hence $\mu_{40} \subseteq X \cap Z$. Furthermore the normal index 40 subgroup Y of X is contained within $\mathrm{SL}_2(\mathbf{F}_{199})$ and hence $\overline{Y} = Y \cap Z$ is a normal subgroup of $\overline{X}$ of index at most 40 and hence a normal subgroup of $\mathrm{PSL}_2(\mathbf{F}_{199})$ of index at most 40. But $\mathrm{PSL}_2(\mathbf{F}_{199})$ is simple and hence $\overline{Y} = \mathrm{PSL}_2(\mathbf{F}_{199})$. This means that Y is either $\mathrm{SL}_2(\mathbf{F}_{199})$ or an index 2 subgroup – but $\mathrm{SL}_2(\mathbf{F}_{199})$ is a perfect group and hence $Y = \mathrm{SL}_2(\mathbf{F}_{199})$, and so $\mu_{40}\,\mathrm{SL}_2(\mathbf{F}_{199}) \subseteq X$. Because we know Y has index 40 in X we deduce that $\mu_{40}\,\mathrm{SL}_2(\mathbf{F}_{199})$ is an index 2 subgroup of X. If $\overline{X} = \mathrm{PSL}_2(\mathbf{F}_{199})$ then this forces $X = \mu_{80}\,\mathrm{SL}_2(\mathbf{F}_{199})$, but this cannot be the case because the eigenvalues α and β of $\rho_f(\mathrm{Frob}_3)$ have the following property: if $\delta \in \mu_{80} \subset \mathbf{F}_{199^2}$ satisfies $\delta^2 = \alpha\beta$ then $(\alpha + \beta)/\delta \notin \mathbf{F}_{199}$. Hence $\overline{X} = \mathrm{PGL}_2(\mathbf{F}_{199})$. □

We finish by remarking that the corresponding $\mathrm{PGL}_2(\mathbf{F}_{199})$-extension of $\mathbf{Q}$ contains a quadratic field J, corresponding to the subgroup $\mathrm{PSL}_2(\mathbf{F}_{199})$. It is easy to establish what this subextension is, as it is unramified outside 2 and 41 and in fact also unramified at 2, because $L/\mathbf{Q}$ is tamely ramified at 2, and hence it must be $\mathbf{Q}(\sqrt{41})$. In particular we deduce the existence of a Galois extension of $\mathbf{Q}(\sqrt{41})$, unramified outside 2 and 41, with Galois group $\mathrm{PSL}_2(\mathbf{F}_{199})$.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478

[Buh78] Joe P. Buhler, *Icosahedral Galois representations*, Lecture Notes in Mathematics, Vol. 654, Springer-Verlag, Berlin, 1978. MR 0506171 (58 #22019)

[Dic58] Leonard Eugene Dickson, *Linear groups: With an exposition of the Galois field theory*, with an introduction by W. Magnus, Dover Publications Inc., New York, 1958. MR 0104735 (21 #3488)

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975). MR 0379379 (52 #284)

[Fre94] G. Frey (ed.), *On Artin's conjecture for odd 2-dimensional representations*, Lecture Notes in Mathematics, vol. 1585, Springer-Verlag, Berlin, 1994. MR 1322315 (95i:11001)

[JR] John W. Jones and David P. Roberts, *A database of number fields*, in preparation. Database at `http://hobbes.la.asu.edu/NFDB/` . Last accessed 27th April 2012.

[Kat77] Nicholas M. Katz, *A result on modular forms in characteristic p*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Springer, Berlin, 1977, pp. 53–61. Lecture Notes in Math., Vol. 601. MR 0463169 (57 #3127)

[Kim94] Ian Kiming, *On the experimental verification of the Artin conjecture for* 2*-dimensional odd Galois representations over* $\mathbf{Q}$*. Liftings of* 2*-dimensional projective Galois representations over* $\mathbf{Q}$, On Artin's conjecture for odd 2-dimensional representations, Lecture Notes in Math., vol. 1585, Springer, Berlin, 1994, pp. 1–36. MR 1322316 (96a:11127)

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. MR 2551763 (2010k:11087)

[S+12] W. A. Stein et al., *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2012, `http://www.sagemath.org`.

[Ser77] J.-P. Serre, *Modular forms of weight one and Galois representations*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 193–268. MR 0450201 (56 #8497)

[Tat76] J. Tate, *Problem 9: The general reciprocity law*, Mathematical developments arising from Hilbert problems (Proc. Sympos. Pure Math., Northern Illinois Univ., De Kalb, Ill., 1974), Amer. Math. Soc., Providence, R. I., 1976, pp. 311–322. Proc. Sympos. Pure Math., Vol. XXVIII. MR 0429839 (55 #2849)

Kevin Buzzard: `buzzard@imperial.ac.uk`.